Exhibit 1

R. Cantor

UNITED STATES DISTRICT COURT

DISTRICT OF MINNESOTA

MDL No. 14-2522 (PAM/JJK)

In Re:	)
TARGET CORPORATION CUSTOMER	)
DATA SECURITY BREACH LITIGATION	)
(This document relates to the	)
Consumer cases.)	)
	)

DEPOSITION OF ROBIN CANTOR, Ph.D.

Washington, D.C.

July 15, 2015

Reported by: Mary Ann Payonk

Job No. 95519

R. Cantor

MR. SEDRAN: Form objection.

MR. MEAL: Let me withdraw that and rephrase it.

BY MR. MEAL:

Q. In terms of that date, September 2, that's far enough out that you're not concerned about taking the Home Depot breach into account for purposes of an analysis such like we see in paragraph 63 --

MR. SEDRAN: Form objection.

Q. -- is that right?

A. I wouldn't say that I'm not concerned, but let me go back again to that decay pattern that you observe.

And within that decay pattern, the amount of fraud that's being reported six months out is much, much smaller than anything you see reported one or two months out. I mean, it's a substantial decay factor.

So the only way you would then worry about the effect of Home Depot is if you were trailing that all the way out past six months into a year, and then yes, what's left in that tail could overlap with Home Depot. I'm not

sure that there would be really any value in counting it because I don't think it would be very much fraud.

Q. What about if it were a fact publicly disclosed that the Home Depot breach in terms of the actual intrusion began in April of 2014? Would that change your view?

A. If I saw information, documents saying that it began in April and the accounts overlapped -- because again, I'm presuming the networks would know if they overlapped -- then I think for the fraud that you start to observe in April and May, that might be something you would look at.

Q. So in that regard --

A. And I do want to say again this is all in the context of this issue of the incremental fraud as opposed to what you might be calculating with total fraud.

Q. Yes, I was just going to ask you a question about the total fraud. So -- and in your methodology in terms of total fraud on the -- what you're calling the compromised accounts, you say that is something that you

think is calculable.

A. Do I think that you can come up with reasonably reliable estimate of the total fraud? Yes, I do. I think you can.

Q. And in your methodology, would you be -- over what period of time would be calculating that total fraud? From when until when?

A. Well, from when to when? I mean, you're asking me a question that I -- the only thing I can tell you right now is that I have six months' worth of data. If I have more information that is given to me, then I -- I would definitely look to see what happens after six months, if I see anything in the tail for the distribution for those accounts.

But there's a reason why it's decaying. It decays because, one, the criminals have already done whatever they're going to do. And two, because the card potentially is reissued now and so that fraud can't be committed on it.

Q. And the six months of data that you have is what?

A. It's the Visa fraud information for six months.

Q. That spreadsheet that we were talking about --

A. Yes.

Q. -- earlier that has the tabs including the tab for Neiman and the tab for Michaels?

A. Yes.

Q. And you don't have any comparable data for MasterCard; right?

A. I do have comparable data for MasterCard, but only for I think it's 82 days' worth of information.

Q. Fair enough. Comparable data durationally speaking. You don't have comparable data durationally speaking for MasterCard?

A. I didn't receive six months of data from MasterCard.

Q. So for purposes of the -- is it fair to say that for purposes of the exercise that you describe in paragraph 63 that the breaches you would look at other than Neiman and

Michaels would be breaches that at least began during the period as to which you're calculating total fraud?

A. I'm sorry, no, I don't -- I didn't understand the question.

Q. Okay, let me break it down. So imagine you've got six months of data on fraud on the compromised accounts and you decide you want to use that as the period with respect to which we're going to calculate total fraud for the purposes of your methodology. Are you with me?

A. Yes.

Q. Okay. So what, if any, relationship would there be if you're going to do that in regard to that six-month period as to the breaches that you'd want to look at for purposes of the exercise that's described in paragraph 63?

A. Again, are you asking me how far back would you go or how far forward would you go? What about you asking me?

Q. How far forward you would go, and particularly, is there a relationship between

how far forward you would go and the period as to which you're calculating total fraud on the compromised accounts. That's really what I'm asking.

A. Well, again, the -- if nothing else happens and the account is part of the compromised accounts and you can -- I mean, I don't understand how you would continue to see fraud on the same account and then nothing is done about it because I do think that once they see fraud on these accounts, they typically do something about it.

But if you're saying no, that they would just let it go, and how far out would I take this, I mean, it can be tracked so could you look, you know, to see at what point does it effectively decay to zero. You could let the data tell you how far out to take things, and then you should be picking up -- as you're doing that, you should be picking up other breaches that might overlap.

But I think that the signal is pretty clear. I mean, the pattern's pretty clear here that it does decay quickly and you wouldn't

expect this to -- I think that makes perfect sense, though, because of what the issuers are doing.

They're just not letting the account sit around and take on more fraud. The customers aren't letting the account sit around, and the card members aren't going to let their account sit around and take on more forward. As soon as that card member understands there's been fraud on the account, they're going to want the account to be reissued. So there's a --

Q. Well, you're -- and that's in regard to an account that suffers fraud. But what about an account that's just been identified as potentially at risk?

A. Yeah, but this is only tracking the fraud that's reported into the system. This isn't making up fraud and putting it in an estimate of fraud for all the compromised accounts; it's only the fraud that's reported into the system. So that's what you're looking at decay.

Q. Correct.

A. We're not -- I mean, I think what you're saying, suggesting, is interesting. You're saying, well, why don't you have an estimate for fraud that might happen on the accounts that you haven't seen yet?

Q. No, I'm just asking -- trying to get an understanding of over what period of time you're anticipating calculating total fraud for purposes of your methodology. The first input in your methodology is total fraud on the compromised accounts, right, so that's going to be total fraud between X date and Y date; right?

A. Right.

Q. I'm asking what you're expecting X date to be and Y date to be, if you know.

A. Well, again, I would generally let the data tell me when things have effectively decayed to zero. So, I mean, I'd have all that information.

Right now, what I have is six months from Visa and I have 82 days from MasterCard. I can look at the patterns from the MasterCard. I can make inferences from the Visa. I hadn't

considered whether or not you might have like a new batch of fraud coming about because of the compromise to cards. But I think you let the data tell you when it seems reasonable to cut this off.

Q. Okay. So what does the data tell you today as to when it would be reasonable to cut it off, that is, what the end date would be for purposes of calculating total fraud for purposes of your methodology?

A. I didn't do a nice smooth curve to tell you what the date is, but I can tell you that six months, it definitely decays and you're at a fraction. I think it might even be only something like 9 percent of what you saw previously for the fraud. So it does decay. The pattern is clear.

Q. And in terms of a start date, what does the data tell you is the start date for purposes of calculating total fraud for your methodology?

A. Well, now, you know, they set a start date. So within their systems, I guess they -- when they do the -- when they have the alerts

Exhibit 2

Account Data Compromise User Guide

15 January 2014

At-Risk Time Frame

When the at-risk start date is known, the fraud recovery formula uses that start date and an end date is determined by using the following table.

If the fraud recovery time frame is not known, the start date will begin 365 days before the date the first MasterCard Alert associated with the case was published and calculate the end date using the following table.

Tier	Minimum Number of Accounts	Maximum Number of Accounts	No. of Days after the Date of MasterCard Alerts Publication
1	5,000,001	Unlimited	60
2	1,000,001	5,000,000	45
3	10,000[5]	1,000,000	30

Refer to the following examples of how the at-risk time frames set forth in the table above are applied.

The following table shows an ADC event with a known at-risk time frame.

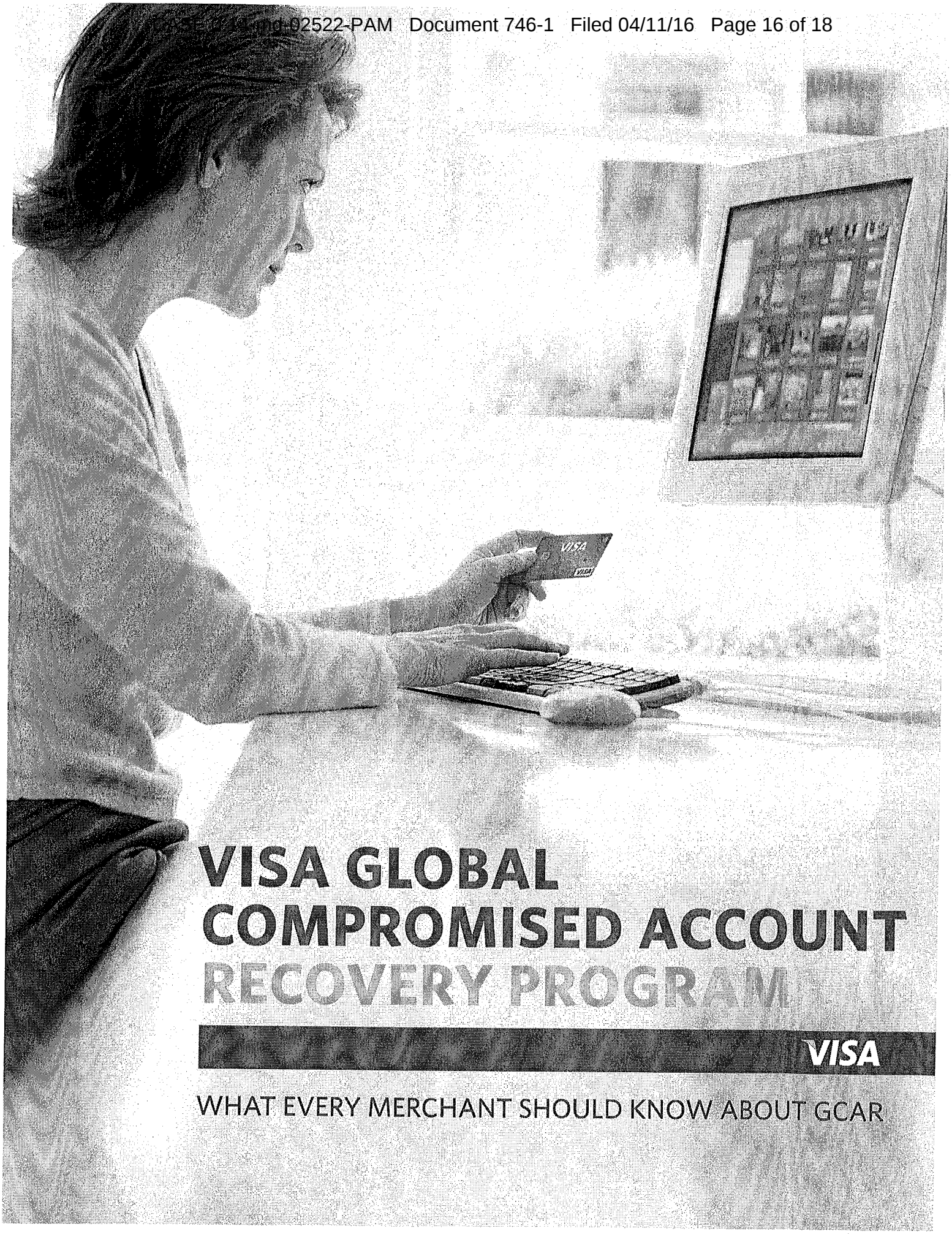
MasterCard Alerts Publication Date	03/01/09
Number of Accounts in the MasterCard Alerts	500,000
At-risk Length	30 Calendar Days (from table above for 500,000 accounts – Tier 3)
At-risk Time Frame—Start Date (Known)	02/01/09
At-risk Time Frame—End Date (Calculated)	03/01/09 plus 30 days = 3/31/09

The following table shows an ADC event with an unknown at-risk time frame.

MasterCard Alerts Publication Date	03/01/09
Number of Accounts in the MasterCard Alerts	500,000
At-risk Length	30 Calendar Days (from table above for 500,000 accounts – Tier 3)
At-risk Time Frame—Start Date (Unknown and Calculated)	02/01/09
At-risk Time Frame—End Date (Calculated)	3/31/09 (03/01/09 plus 30 days)

5. MasterCard reserves the right to invoke FR for cases that are less than 10,000 accounts.

Exhibit 3



VISA GLOBAL COMPROMISED ACCOUNT RECOVERY PROGRAM

VISA

WHAT EVERY MERCHANT SHOULD KNOW ABOUT GCAR

- Determine Incremental PIN Counterfeit Fraud

  Issuer-reported magnetic-stripe PIN counterfeit fraud minus baseline PIN counterfeit fraud = **incremental PIN counterfeit fraud** (on eligible accounts included in the event IC and/or RA CAMS Alert(s)).

  FOR EXAMPLE:

US $2,000 (issuer PIN counterfeit fraud) minus US $1,000 (baseline PIN counterfeit fraud)	=	US $1,000 of incremental PIN counterfeit fraud

How the Fraud Window Affects the Calculation

The Incremental Counterfeit Fraud liability calculation includes only the fraud that has occurred during the Fraud Window. The Fraud Window begins up to 365 calendar days prior to and 30 calendar days after the Fraud Window Anchor Date. The Fraud Window cannot begin before the start of the Intrusion Access Window. Visa may elect to adjust the Fraud Window start and end dates[11] (e.g., if non-cooperation significantly increases amount of time required to complete the investigation).

Key Points to Remember About the Incremental Counterfeit Fraud Recovery Calculation

- If a PIN compromise is involved in an event, a separate PIN counterfeit fraud baseline calculation will be used.
- A Fraud Window associated with each Fraud Window Anchor Date is a maximum of 365 calendar days plus 30 calendar days. It begins with the earliest known exposure, not to exceed 365 calendar days prior to the Fraud Window Anchor Date, and concludes 30 calendar days following the Fraud Window Anchor Date.
- Accounts will be excluded from the Incremental Counterfeit Fraud recovery calculation if they were sent within the prior 180 calendar days in another IC and/or RA CAMS alert indicating magnetic-stripe data was At-Risk. Fraud that is reported after the fraud reporting deadline applicable to the issuer's region is not eligible for recovery.
- Fraud transactions that were not reported through Visa's Fraud Reporting System (FRS) will be excluded from Incremental Counterfeit Fraud Calculations. Visa will exclude from its calculation of the Incremental Counterfeit Fraud amount any transactions that were successfully charged back by the issuer and for which the acquirer did not submit a successful representment at the time of the calculation.
- For Account Data Compromise Events with Compromised Locations outside the United States Region, fraud reported on accounts that were authorized through VisaNet in a transaction

[11] These adjustments will never cause the Fraud Window to exceed 365 calendar days plus 30 calendar days.

processed through one or more of those Compromised Locations will be eligible for GCAR recovery.

- If an Account Data Compromise Event involves Compromised Locations both inside the United States Region and outside the United States Region, for GCAR Incremental Counterfeit Fraud and Operating Expense Recovery calculation only, the event can be divided into separate calculations to accommodate VisaNet authorization verification for the segment of accounts put At Risk at non-US Compromised Locations.

Issuer Operating Expense Recovery Calculation

Calculation for determining Operating Expense Recovery

- The GCAR Program sets Operating Expense Recovery at US $2.50 per eligible account.
- For events that would otherwise qualify for the GCAR program, Visa will also provide operating expense compensation for issuers of US $2.50 per additional eligible account for each account with compromised PAN and CVV2 data in an Account Data Compromise Event involving a VisaNet processor, agent or payment facilitator.

Note: To qualify as a GCAR event, the compromise must also affect at least 30,000 PAN and CVV eligible compromised accounts and have a liability assessment of more than U.S. $300,000.

Key Points to Remember About the Operating Expense Recovery Calculation

- Accounts are excluded from the Operating Expense Recovery calculation if they were sent within the prior 180 calendar days in an IC and/or RA CAMS alert indicating magnetic-stripe data was At-Risk.
- For Account Data Compromise Events with Compromised Locations outside the United States Region, to be eligible for Operating Expense Recovery, accounts must have been authorized through VisaNet in a transaction processed through one or more of those Compromised Locations.
- If an Account Data Compromise Event involves Compromised Locations both inside the United States Region and outside the United States Region, for GCAR Incremental Counterfeit Fraud and Operating Expense Recovery calculation only, the event can be divided into separate calculations to accommodate VisaNet authorization verification for the segment of accounts put At Risk at non-US Compromised Locations.

Issuer Recovery Amount for Capped Cases

The total issuer recovery amount for an event is allocated by issuer BIN. This allocation is based on the issuer BIN's proportional share of the fully calculated Operating Expense Recovery, plus the Incremental Counterfeit Fraud amounts before the liability cap has been applied.